Robot Zertifikate - Policy und erste Erfahrungen

Bernadette Fritzsch, AWI

für das GapSLC Team

Use Case

- Nutzung von definierten Diensten im Grid mit unkritischen Daten
- Anwendungsfälle aus den Communities
  - Zugriff auf veröffentlichte Dokumente (TextGrid) bzw. frei zugängliche Klimadaten (C3Grid)
  - Verteilung von embarrisingly parallel Jobs (AstroGrid)
  - Analyse von Verwandtschaftsbeziehungen zwischen Tier-Genomen (MediGRID)
  - Zugriff auf frei zugängliche biomedizinische Ontologien (MediGRID)
- Automatisierte Dienste (user level monitoring, dg-ops)

Absicherung von spezifischen Diensten

Zuordnung des jeweiligen Jobs auf konkreten Nutzer bei bestimmten Anwendungen nicht notwendig oder wünschenswert

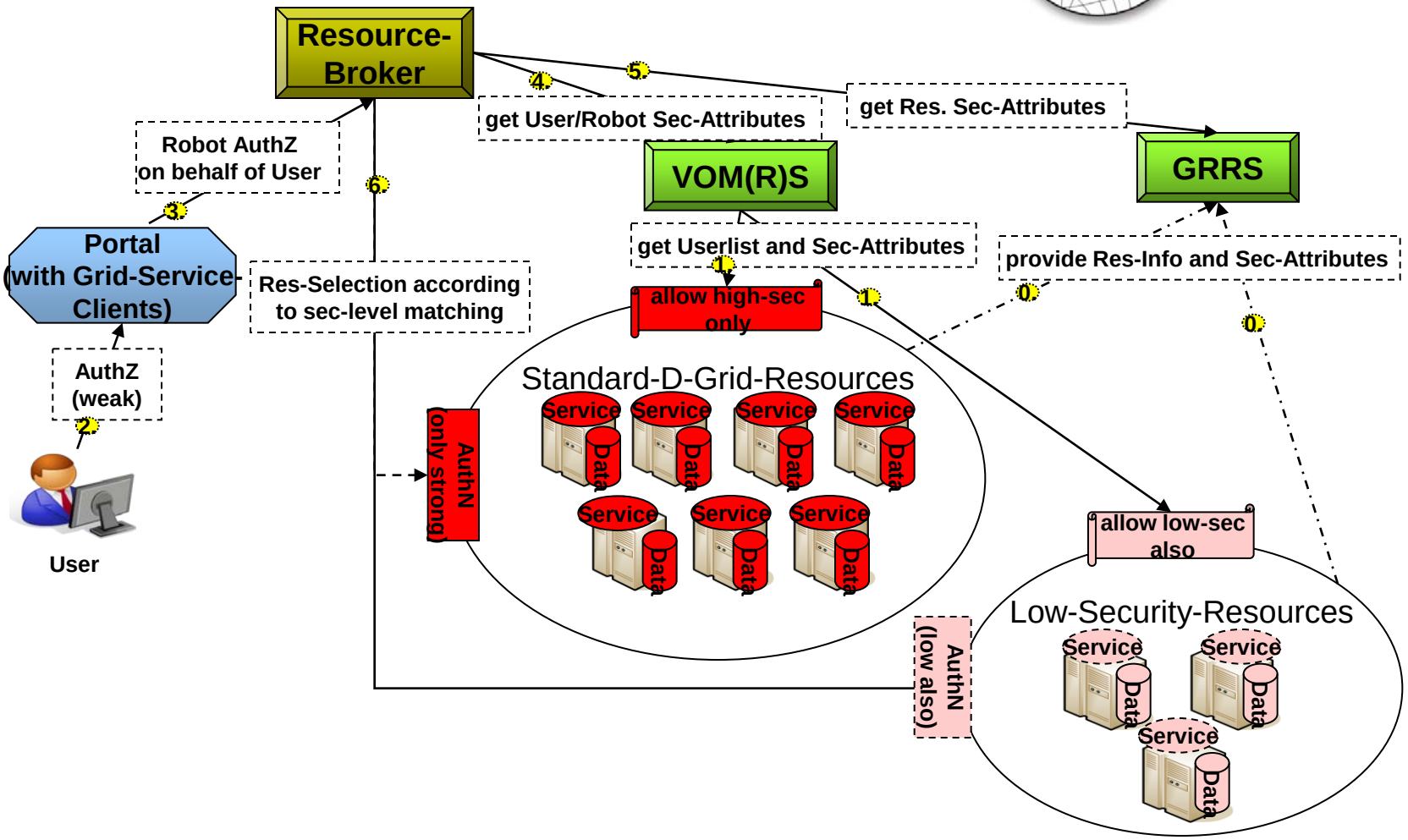
- Insellösungen in den Communities
  - Dienstezertifikate durch community-interne Policy abgedeckt
  - Auf allgemeinen D-Grid Ressourcen nicht anwendbar
- Wunsch nach Erweiterung der D-Grid Policy
  - Konzept in GapSLC entwickelt
  - DFN-PKI erweitert (EUGridPMA)

Policy

- Zuordnung von x509-Zertifikate zu einem Dienst (Diensteanbieter)
- Anpassung der DFN-PKI in Abstimmung mit EUGridPMA : automated clients
  - Kennzeichnung als Robot-Zertifikat
  - Persistente Gruppe von Verantwortlichen → email-Adresse (Vertreter!)
  - Vorkehrungen zur Verwahrung des persönlichen Schlüssels (Krypto-Token/Hardware Security Module oder gesicherter Rechner, Zugang zum Rechner, Zugriff nur von verantwortlichem Personenkreis; …)
- Nutzungskonzept:
  - getrennte Ressource-Pools mit unterschiedlichen Security-Leveln bei den RP
  - Diskussion mit RPs (OIS AHM)inzwischen (teilweise) in Policy enthalten

    → Siehe „Erweiterung VO-Konzept“ (DGI FG 2.7)

Policy


Resource-Broker
get User/Robot Sec-Attributes
get Res. Sec-Attributes
Robot AuthZ on behalf of User
VOM(R)S
GRRS
Portal (with Grid-Service-Clients)
get Userlist and Sec-Attributes
provide Res-Info and Sec-Attributes
Res-Selection according to sec-level matching
allow high-sec only
AuthZ (weak)
Standard-D-Grid-Resources
Service
Data
AuthN (only strong)
allow low-sec also
Low-Security-Resources
AuthN (low also)
User

Erste Erfahrungen in TextGrid

- Abgesicherter Dienst für Dateioperationen TG-crud (create, read, update, delete):
  - Lesen von veröffentlichten Dokumenten durch anonyme Nutzer
  - Lese- und Schreiboperationen auf Dokumenten durch schwach authentifizierte Nutzer (E-Mail- Verifikation)
- Autorisierung geschieht über separate Zugriffskontrolle (TG-auth* mit openRBAC)
- Erfüllung der Vorgaben der Grid-PMA
  - Besonderes Format des Zertifikats (Aufbau des subjectDN, Mail im SubjectAltName) → als Robot erkennbar
  - Erstellung einer Sicherheitspolicy für die konkrete Rechner- und Organisationsumgebung (Virtualisierung, Portfreigabe, …) → Dokument
  - Absicherung des Rechners gegen Schlüsselmissbrauch anhand der Policy

Ausblick - Offene Probleme

- Erfahrungen mit Robot-Zertifikaten
  - Konzept und prototypische Umsetzungen in GapSLC
  - Jetzt Ausweitung der community-internen Praxis auf D-Grid Ressourcen möglich
  - Bereitstellung der Dokumente/Erfahrungen für andere Communities
- Aufwand: Nutzer ↓, Diensteanbieter ↑
- Ausweitung
  - Schnittstellen GRRS, VOMRS für Security Level
  - Akzeptanz bei Ressourcenanbietern